安装与卸载

这一部分介绍了旁路分析工具箱（Side-Channel Analysis Toolbox）的几种安装和卸载的方法。

Contents

MATLAB 安装一个工具箱的方式主要有两种：

1. 通过工具箱文件（.mltbx 格式）安装
2. 将源文件添加到 MATLAB 搜索路径

因此下面列举的几种不同安装方法，都是这两种方法的延伸和变化，本质上没有区别。

事实上，通过工具箱文件安装，也只是将打包好的源文件解压到 MATLAB 的搜索路径中。

安装方法1：使用 Add-On Explorer

由于本工具箱已经通过 MATLAB File Exchange 平台发布，因此你可以直接在 MATLAB 自带的 Add-On Explorer 中找到本工具箱并安装。 操作如下：

1. 进入 MATLAB 主界面，点击 Apps > Get More Apps，弹出窗口：Add-On Explorer
2. 在搜索框输入：scatool，回车
3. 搜索到 scatool 后，点击进去可以看到简介：Side-Channel Analysis Toolbox，以及一些基本信息
4. 点击右上角的 Add，MATLAB 将自动帮你安装工具箱，无需后续操作

这个方法简单快捷，推荐新手使用。

安装方法2：使用 File Exchange 平台

File Exchange 是 MATLAB 的一个开源社区，用户可以在上面分享和下载代码。

本工具箱的下载地址是： https://cn.mathworks.com/matlabcentral/fileexchange/66698-scatool

在浏览器中复制粘贴该链接，跳转到对应的页面，这个页面和你在 Add-On Explorer 里看到的非常类似。

（或者你也可以到主页中搜索 scatool： https://cn.mathworks.com/matlabcentral/fileexchange/）

点击右侧的 Download，选择下载 Toolbox 或者 Zip。

如果你选择了下载 Toolbox，那么可以按照如下方式安装：

1. 在 MATLAB 中进入下载的 scatool.mltbx 所在的文件夹，这时在侧边栏 Current Folder 中可以看到这个文件
2. 双击 scatool.mltbx 即可完成安装。

这个方法和上面的方法类似，只不过获得文件的途径有所不同。可以作为备选方案。

如果你选择了下载 Zip，那么可以如下方式安装：

1. 在自己喜欢的路径下解压该 zip 文件
2. 进入 MATLAB 主界面，点击 HOME > Set Path > Add with Subfolders
3. 选中解压了的文件的父目录 scatool
4. 点击 Save，再点击 Close，即可完成安装

这个方法较为复杂，需要 MATLAB 的文件路径搜索机制有一定的了解，不推荐使用。

安装方法3：使用 GitHub

本工具箱使用 GitHub 进行版本管理，因此你也可以通过这种途径下载到文件。

本项目 Release 的地址为： https://github.com/Hansimov/scatool/releases

在这个页面你可以看到本工具箱的历史版本，建议选择最新的版本。

可以下载的文件有两种： Source Code （.zip/.tar.gz）和 scatool.mltbx。

scatool.mltbx 的内容和上面两类方法中提到的一样。 文件下载后，安装方式和方法 2 中相同。

这个方法也可以作为备选方案。

如果你好奇心比较强烈，下载了 Source Code，那么这里也做一下简单的说明和提醒。

如果你将解压后的文件都添加进 MATLAB 的路径中，也相当于安装了这个工具箱。

不过，需要注意的是，其内容和 File Exchange 上下载到的 zip 文件大为不同。 Source Code 中不仅包含了项目中可用的部分，也包含了一些正在开发和测试的文件。 那些正在开发和测试的文件，体积远比正式发行的要大。

因此，开发者的忠告是，大多数时候，不必下载 Source Code。

卸载是安装的逆过程。方法和思路与安装类似。

（一个不能完整卸载的软件不是一个好软件。）

卸载方法1：使用 Add-On Manager

如果你是通过上面的方法 1 或者是 scatool.mltbx 文件安装的，那么卸载方法也很简单。操作如下：

1. 进入 MATLAB 主界面，点击 HOME > Add-Ons > Manage Add-Ons，弹出窗口：Add-On Manager
2. 找到工具箱 scatool，然后点击右侧的 Uninstall，即可完成卸载。

这个方法简单快捷，推荐新手使用。

卸载方法2：删除文件和 MATLAB 搜索路径

如果你使用安装方法是将文件添加进 MATLAB 搜索路径，或者不信任 MATLAB 的 Add-On Manager 已经把该工具箱删干净了，那么你可以手动删除该工具箱的所有文件。

如果你使用的是双击 scatool.mltbx 安装，那么采取如下操作卸载：

1. 进入 MATLAB 主界面，点击 HOME > Preferences > MATLAB > Add-Ons，这里你可以看到自己的 Add-On 默认安装的路径
2. 通过文件浏览器进入该文件夹，然后删除 scatool 以及其下的所有文件
3. 进入 MATLAB 主界面，点击 HOME > Set Path，选中那些和 scatool 有关的路径 （可以按住 ctrl 独立选中，或者按住 shift 批量顺序选中），点击 Remove，即可
4. 如果你懒得挨个选中路径并删除，那么直接点击下面的 Default，将 MATLAB 的文件路径还原到初始状态即可。

如果你以前添加过其他文件夹的路径，那么请谨慎使用这个方法。

如果你是用解压 zip 文件并添加路径的方法安装，那么只要进入当初解压到的文件路径，执行上述 2~4 的步骤即可。

Published with MATLAB® R2017a

图形用户界面的使用

图形用户界面（Graphical User Interface）和命令行界面（Command-Line Interface）是两种常见的软件用户界面。 对于新手来说，图形界面往往比命令行更友好。 因此本工具箱提供了一个图形界面，用于帮助初学者更快地熟悉旁路分析的流程。

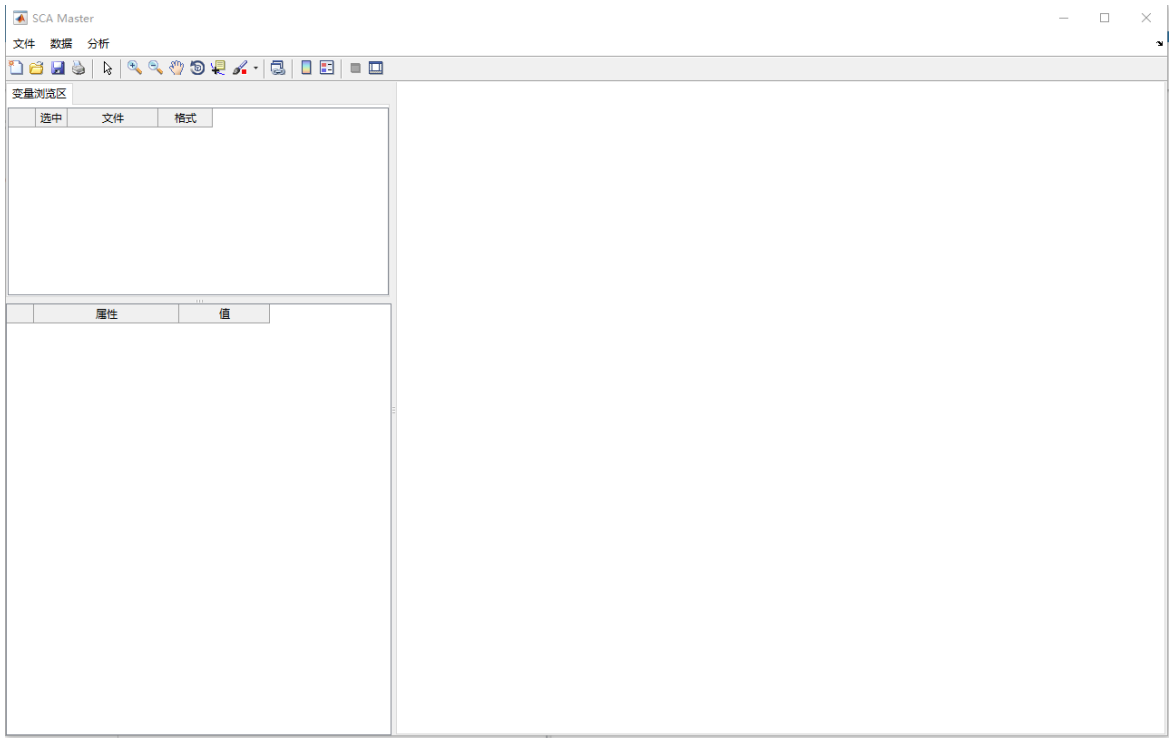
Contents

图形界面的启动

启动图形界面很简单，只需要在 MATLAB 的 Command Window 中输入如下命令：

```
scamaster
```

稍等几秒，你就能看到如下界面：



界面有如下几个部分：

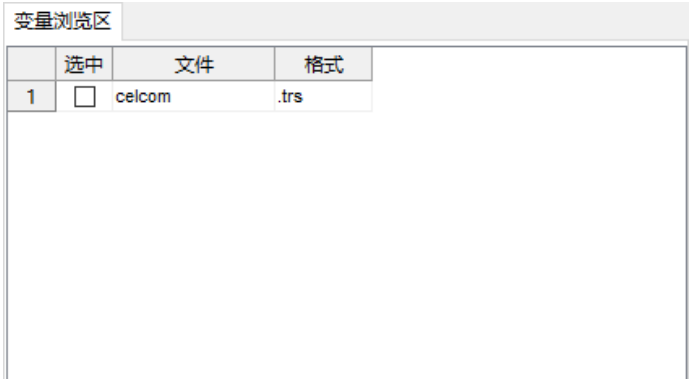
- 菜单栏（上方）：用于执行一系列针对功耗曲线的操作，比如导入、查看和分析
- 变量浏览区（左上）：可以查看当前导入的功耗曲线文件和正在的中间曲线
- 信息展示区（左下）：展示所选功耗曲线文件的相关细节
- 曲线绘制区（右侧）：绘制并查看曲线

导入功耗曲线

假定你现在已经通过设备采集了硬件的功耗曲线，其格式为 .trs。你可以通过如下方法导入该曲线：

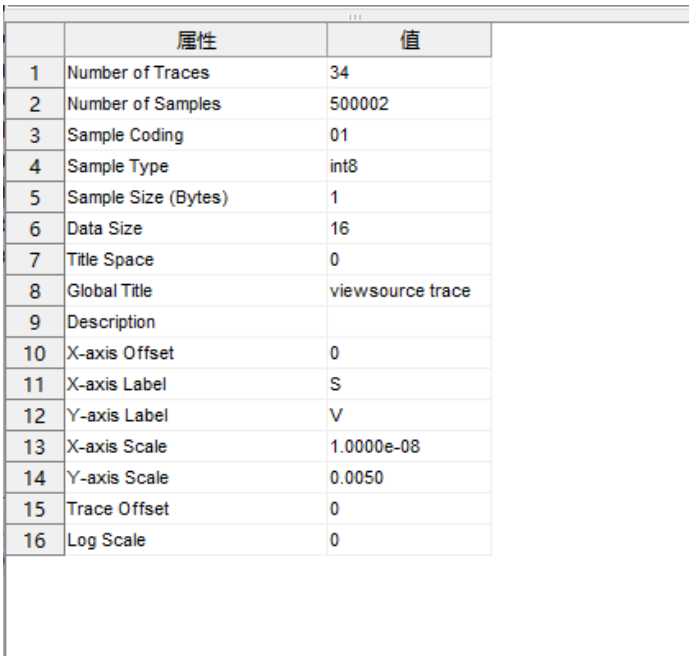
1. 在菜单栏中点击：文件 > 导入
2. 这时会弹出文件选择的窗口，你可以选择一个或多个采集到的功耗曲线文件。

导入曲线后，变量浏览区如下所示：



曲线的基本信息

在变量浏览区，单击新增的曲线所在行，你会发现下面的信息区表格中出现了该文件的一些基本信息。



	属性	值
1	Number of Traces	34
2	Number of Samples	500002
3	Sample Coding	01
4	Sample Type	int8
5	Sample Size (Bytes)	1
6	Data Size	16
7	Title Space	0
8	Global Title	viewsource trace
9	Description	
10	X-axis Offset	0
11	X-axis Label	S
12	Y-axis Label	V
13	X-axis Scale	1.0000e-08
14	Y-axis Scale	0.0050
15	Trace Offset	0
16	Log Scale	0

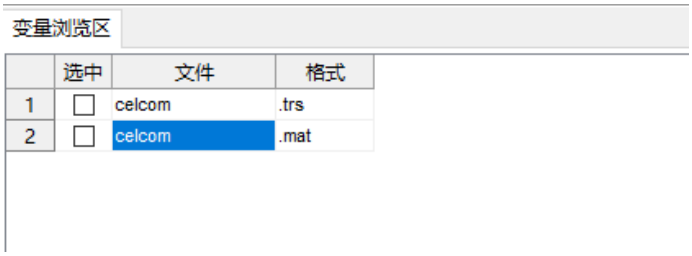
这些信息包括：文件中曲线的条数、每条曲线的样本点数、样本点的数值格式，等等。

我们在后续处理这些曲线时，这些信息会很有用。

.trs 格式转为 .mat 格式

设备采集得到的功耗曲线文件一般是 .trs 格式的，而适合 MATLAB 处理的是 .mat 格式。 因此需要将 .trs 格式的文件转换成 .mat 格式。 操作方法如下：

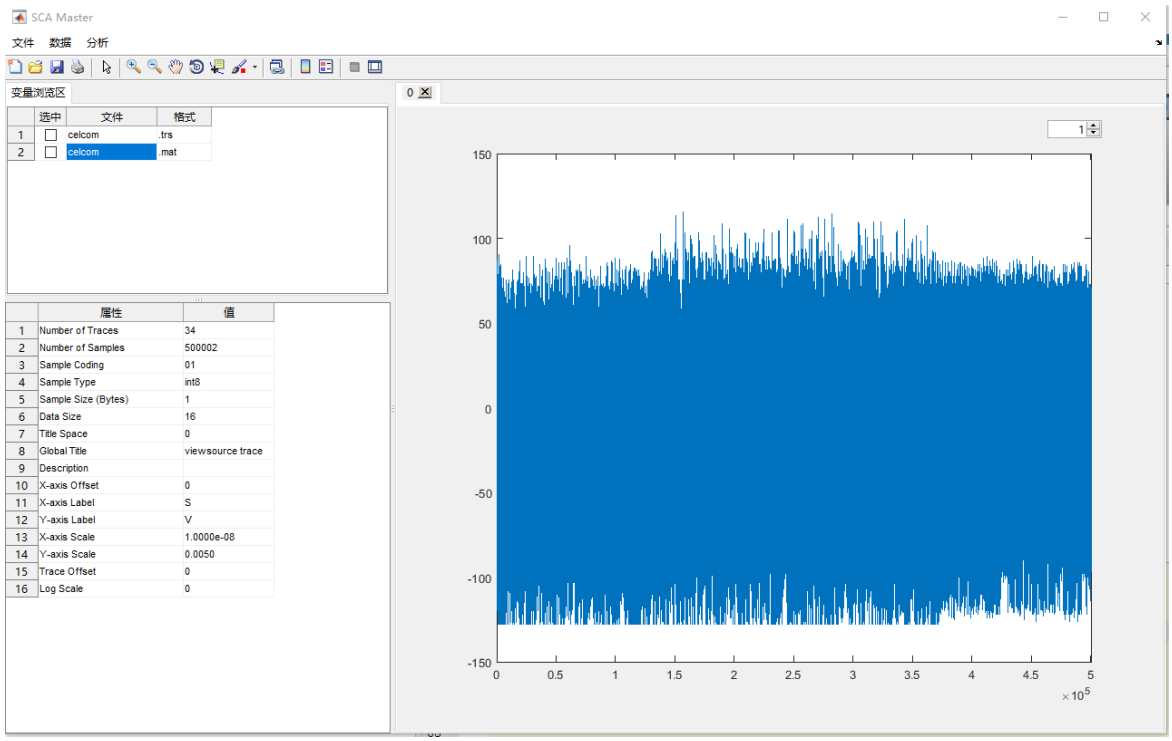
1. 在变量浏览区左键单击该曲线所在行，右键选择“转换成 .mat 格式”
2. 这时会弹出文件保存的窗口，你可以重命名该文件以符合习惯，点击“确定”开始转换
3. 转换完成会提示是否打开转换后的 .mat 文件
4. 如果选择打开，你将看到变量浏览区多了一行，其格式为 .mat



查看曲线

得到 .mat 格式的文件后，我们选中新增的这一行，右键，可以看到我们能实施的操作变多了。

我们选择“查看曲线”：



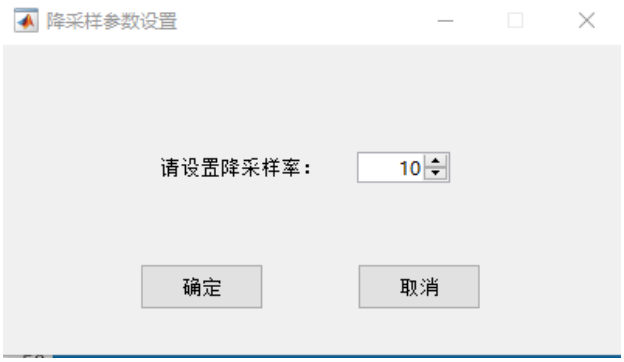
右上角旋钮中显示的是当前所查看的曲线是第几条。

你可以点击按钮，查看上一条或下一条曲线；也可以直接输入数字，跳到对应曲线；还可以通过键盘的上下方向键，切换查看的曲线。

降采样

有时候，我们每条曲线采的样本点数过多，数据量很大，处理时不仅耗时，而且还可能造成内存溢出。 因此我们有必要对功耗曲线进行降采样，以减少每条曲线的样本点数，提高后续处理的效率。

仍然是单击想处理的曲线所在行，右键选择“降采样”，这时会弹出“降采样参数设置”的界面。

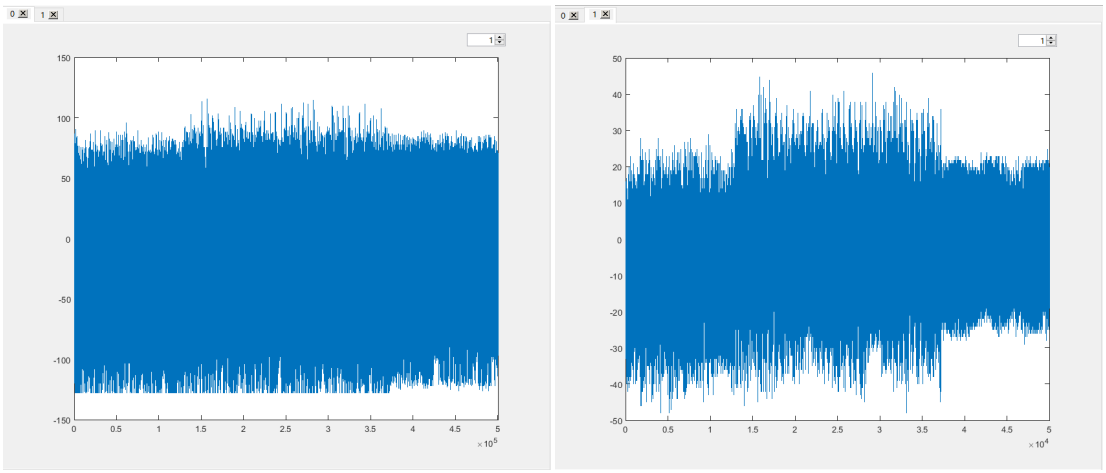


这里的“降采样率”指的是曲线数目减少的倍数。比如采样率设置为10，那么假设原先每条曲线有10000个点，降采样完就是1000个点。

选择适合的降采样率，点击“确定”。

这时我们可以看到变量浏览区又多了一行，并且文件名后面多了“_ds”。“ds“是 down sample（降采样）的首字母缩写。

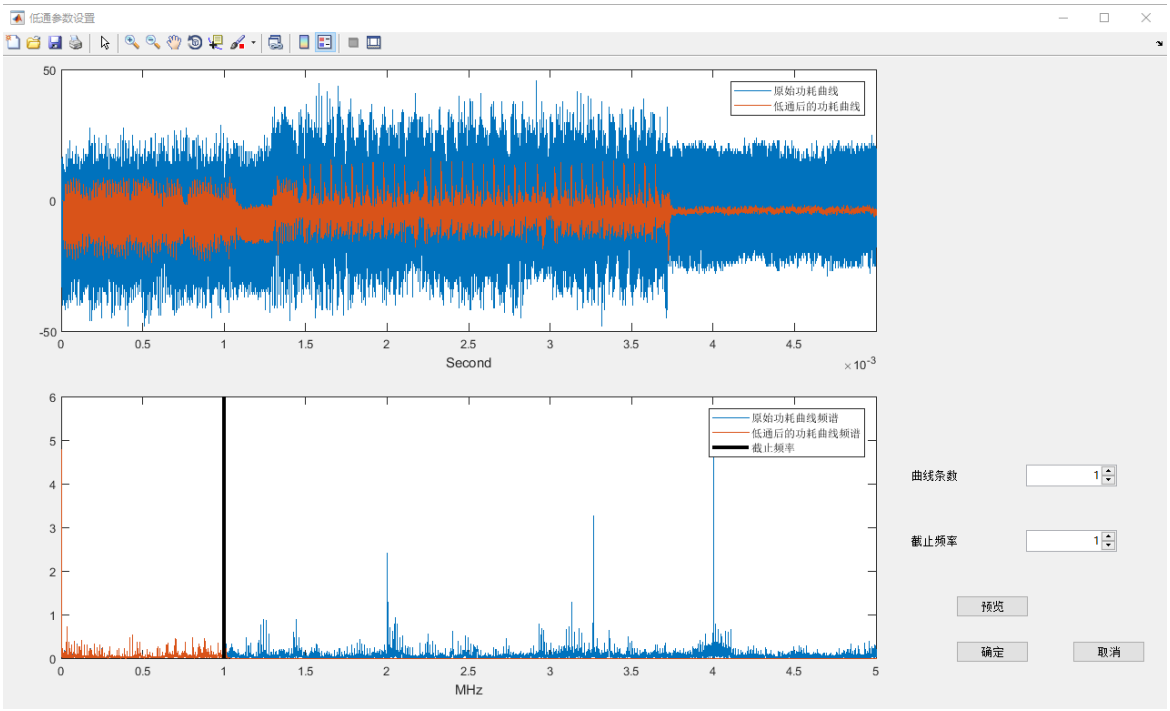
从图中可以明显看出降采样前后曲线的粒度变化。



低通

采集到的曲线往往会混有很多噪声，这些噪声大多数都处在高频部分，对我们的功耗分析产生干扰。 对曲线进行低通，可以滤掉大部分噪声，提高处理的效率和精度。

单击降采样后的曲线，右键选择“低通”。稍等几秒，便会弹出低通参数设置的窗口。



上方的图像展示了功耗曲线的时域信息，下方的图像呈现了频域信息。

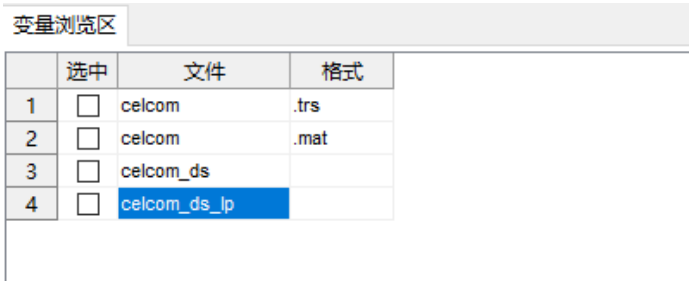
你可以设置右侧“曲线条数”的值，来查看不同曲线的时域和频域信息。

拖动频域图像中黑色的粗线，来设置低通的截止频率；也可以通过设置右侧“截止频率”中旋钮的值，实现同样的效果。

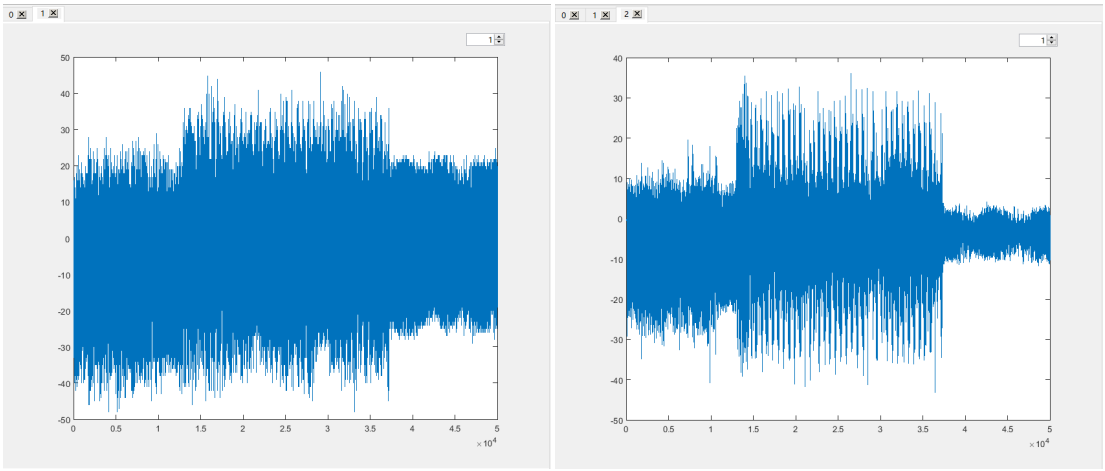
调整好截止频率后，可以点击“预览”，查看新的截止频率对曲线产生的影响。 需要注意的是，由于低通操作需要耗费一定的时间，因此尽量避免频繁地点击预览。

如果调整完成，点击“确定”，软件就会按照你设置的参数对曲线进行低通。

这时我们可以看到变量浏览区又多了一行，并且文件名后面多了“_lp”。“lp“是 low pass（低通）的首字母缩写。



从图中可以明显看出低通前后曲线的粒度变化。



对齐

由于各种原因，硬件设备采集到的不同功耗曲线并不是严格对齐的。 这句话的意思是，在采集到的不同曲线的相同时刻，对应的实际程序指令并不相同。 如果功耗曲线之间没有对齐，就无法进行有效的差分功耗分析。 因此，我们需要对将要攻击的区域进行对齐，以保证同一时刻，对应的程序指令是相同的。

攻击

在对曲线进行了上述各种预处理之后，我们就可以对曲线实施差分功耗分析了。

Published with MATLAB® R2017a

常用函数和模块

除了提供的图形用户界面外，旁路分析工具箱还提供了一些常用的函数和模块。 这些预置的函数和模块，可以让用户专注于设计算法的关键部分，而不必在无关紧要的细枝末节上花费过多的时间从而更快更好地验证自己的想法。

一些常见的函数和模块如下。

Contents

数据类型转换

密码算法

Published with MATLAB® R2017a

反馈和帮助

本工具箱目前（2018.03）尚处在早期开发和测试阶段，有很多功能还不完善。

如果你在使用过程中遇到问题，或者有新的想法，可以通过以下途径获得支持和帮助。

Contents

邮箱

开发者的邮箱为： zehan.yu@viewsources.com

我们会尽快回复你的反馈和疑问。

群聊

很多时候，发送邮件无法得到及时的答复，交流的效率也相对较低。 因此你可以加入 QQ 群以获得更快速和更详细的支持和帮助。

QQ 群：旁路分析技术交流群

群号：725662287

二维码：（是的，我们是如此的与时俱进）

GitHub

如果你在使用工具箱的过程中有新的需求，或者出现了问题或者错误（我相信这不仅会发生，而且会很频繁），最好的方法是到 GitHub 上提交一个 issue。

在 GitHub 上提交 issue，往往比在 QQ 群里询问开发者更有效。 原因在于，作为一个软件开发者，很可能会对千篇一律地教人们如何使用软件感到厌烦，但绝对不会在软件出错时坐视不管。

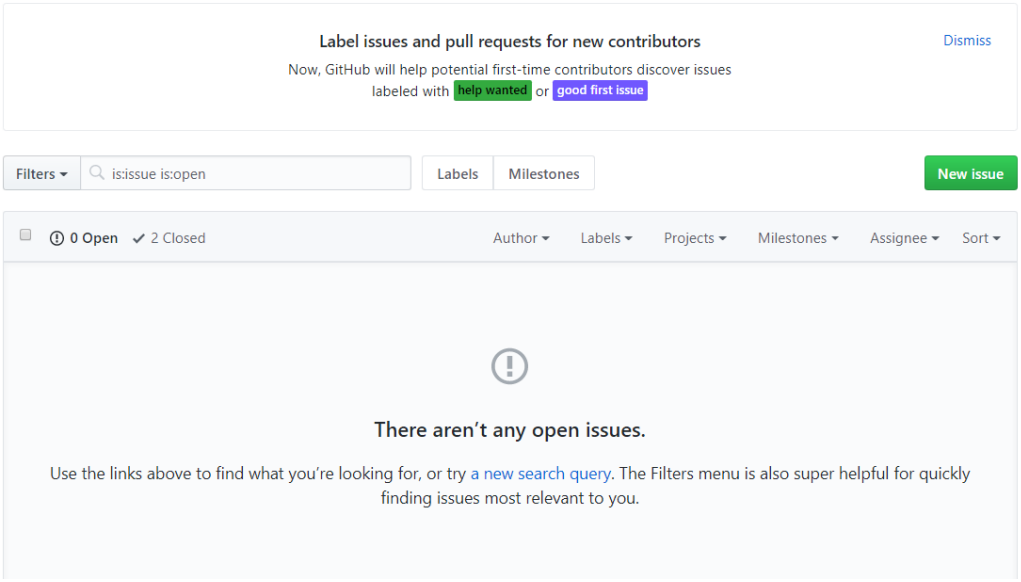
与此同时，GitHub 的 issue 对所有人可见，并且可以留存足够长的时间。 你在今天碰到的问题，很可能半年后的另外一个人也会碰到。或者相反地，你半年后碰到的某个问题，很可能半年前有人已经碰到过了。

如果问题的解决方案在第一时间以书面的形式记录了下来，不但能省去很多沟通的成本， 也能极大地提高解决问题的效率，更能造福后人，不用再走一遍弯路。何乐而不为呢？

不过，你可能有点担心，因为你甚至都没听说过 GitHub，即使有所耳闻，也从来没有用过。 丝毫不用担心，只要简单几步，你就可以完成问题的提交。

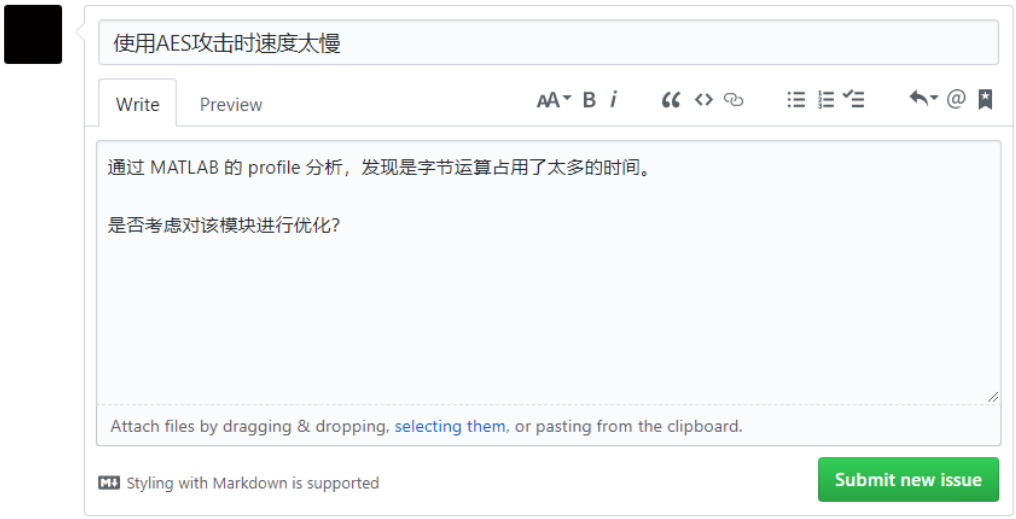
首先，提交 GitHub issue 的地址是： https://github.com/Hansimov/scatool/issues

然后，点进去你将看到这样一个界面：



如果你还没有 GitHub 账号，可以注册一个（很快的），否则无法提交问题。如果你看到这里决定放弃了，那也没关系，懒人自有懒福。

如果你已经有了 GitHub 的账号，那么可以在上述页面中，点击右侧的“New Issue”，这时你会跳转到另一个页面。 此时，你就可以表述你的问题：



点击“Submit new issue”，即可完成问题的提交。

不过既然你已经看到这里了，一定不介意再多看两句。

一个好的提问，应当尽可能提供问题出现时的环境和细节，这有利于开发者和别的使用者更好地定位问题的原因。

此外，在提问之前，最好能够搜索一下，是否已经有类似的问题，避免重复。

当然，好的提问还需要具备很多其他的因素，不过只要遵循上面提到的两点，就已经足够了。

最后，希望这个工具箱能够对你有所帮助。

Published with MATLAB® R2017a